Remarks

Claims 1-32 are pending in the present application. Claims 27 and 32 have been amended. Support for the amendment to claims 27, 32 may be found, for example, at page 6, lines 23-25.

35 U.S.C. §101

It appears from the office action that at least some claims were rejected under 35 U.S.C. §101 because the computer program product recited in the claims is *per se,* not on a computer readable medium. The Examiner did not identify the specific claims under rejection. However, in an effort to advance prosecution of the instant application, the applicants have amended the computer program product claims 27 and 32 to recite that the program code is on a computer usable storage medium. If the Examiner intended to reject other claims, then applicants respectfully request that the specific claims being rejected are identified so that the applicants can respond appropriately. In view of the amendments herein, the applicants respectfully request that the rejection to claims under 35 U.S.C. §101 be withdrawn.

35 U.S.C. §103

Claims 1-3, 5, 7-11, 14, 15 and 26-32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over WO 99/56194 to Bartolomeos *et al.* (hereinafter '*Bartolomeos*') in view of U.S. Pat. Pub. No. 2001/055388 to Kaliski, JR. (hereinafter '*Kaliski*'). According to the M.P.E.P. §706.02(j), to establish a *prima facie* case of obviousness, the prior art reference must teach or suggest all the claim limitations. It is the applicants' position that the art does not support the rejections to the claims herein, thus a *prima facie* case of obviousness has not been established. Accordingly, the applicants respectfully request that the above rejections are withdrawn.

With respect to claim 1, *Bartolomeos* in view of *Kaliski* fails to teach or suggest at least:

> A method for a middle-tier server to impersonate a client to a plurality of servers … comprising …obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers …

In the Office action, the Examiner correctly points out that *Bartolomeos* fails to teach or suggest that the disclosed authentication data utilizes a common nonce associated with each of the plurality of servers as claimed[1]. In this regard, the Examiner relies upon the teaching of *Kaliski*. However, the applicants assert that obtaining a common nonce as claimed, is also completely missing from the teaching or suggestion in *Kaliski*. As such, the applicants respectfully traverse the above rejections.

As will be described in greater detail below, the invention in *Kaliski* utilizes a plurality of unique and individual nonces as part of a verification process to confirm that strong secret data has been properly recovered, and does not teach or suggest a common nonce associated with a plurality of servers as claimed. Moreover, *Kaliski* explicitly and expressly teaches that each independent nonce can only originate from one of two sources including the client or the corresponding server. As such, the claimed method comprising obtaining a common nonce associated with each of a plurality of servers from an entity other than the client or the plurality of servers cannot reasonably be construed to read on the server assisted regeneration of strong secret data from a weak secret as taught in *Kaliski* as will be described in greater detail below.

The invention in *Kaliski* is directed to allowing a user to obtain strong secret data, e.g., a cryptographic key, as a function of a user's weak secret data, e.g., a password in combination with server secret data[2]. For example, the user may be at a public terminal and may not know the strong secret data. However, using a password, the user can securely recover and reconstruct the strong secret data, e.g., to digitally sign messages, etc.[3] from data segments that are distributed across a plurality of servers.

In general, strong secret data, designated K, is a function of the user's password and a plurality of "server data segments", i.e., server secret data, designated b(i), where (i) is an index corresponding to a different server of a plurality of servers S(i). In this regard, the server secret data is deliberately split up to a plurality of separate servers to

[1] See Office action mailed 06/04/2007, page 5.
[2] See for example, *Kaliski*, paragraph 16.
[3] See for example, *Kaliski*, paragraph 49.

avoid the potential that someone "hack" enough information so as to be able to reconstruct or otherwise guess the user's strong secret data. As noted in *Kaliski,* it is "important" that messages exchanged between the client and each server S(i) be authenticated and that the integrity of these messages is maintained[4]. For example, the servers may be (and are preferably) controlled by different entities so that no individual entity has access to all of the servers 130[5] (or data thereof). Regardless of how each server stores its corresponding server data, only the generating client has access to the final strong secret data K. Once the generating client recovers the user's strong secret data K, a recovery system verifies that the strong secret data K was recovered properly. The recovery process is of relevance to the analysis herein.

In making the rejection, the Examiner argues that *Kaliski* teaches that a client signs a message containing "…a nonce from each of the servers…"[6]. However, this fails to teach or suggest obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers as is claimed.

Firstly, each nonce N(i) comes from its corresponding server directly or from the client side verification process, e.g., the recovery client 220, and thus the claimed invention cannot read on the invention described in *Kaliski*. Moreover, as noted in *Kaliski*, assuming that each server S(i) has authenticated the user, each server computes its own unique server response data C(i)=M(i) (see 630) and sends C(i) to the recovery client 220 (see 635). Each server[7] also generates a unique index N(i), or nonce, for this instantiation of the recovery process and transmits the nonce to the recovery client 220[8]. As such, *Kaliski* fails to teach or suggest a common nonce associated with each of a plurality of servers because, contrary to that claimed, each server generates and independently transmits its own nonce directly to the client.

---

[4] See for example, *Kaliski*, paragraph 55.
[5] See for example, *Kaliski*, paragraph 47.
[6] See the Office action mailed 06/04/2007, page 5, lines 14-19.
[7] See for example, *Kaliski*, paragraph 51 "Each of the dashed boxes 110, 120, 130, 140, and 220 represents one of the components of system 100 or system 200. The solid boxes represent various steps in the two methods 300 and 400. The location of a solid box within a dashed box generally indicates that that specific step is performed by that specific component."
[8] See for example, *Kaliski*, paragraph 83.

The recovery client 220 generates proof data at 650 by digitally signing a message for each server S(i) using the user's recovered private key, where each message includes the associated nonce N(i). Correspondingly, each server verifies successful recovery of the strong secret data K by decoding the digital signature using the user's public key and by verifying that the correct nonce N(i) is included in the decoded message. A similar result may be realized using hash functions. Thus, the recovery client 220 generates a plurality of messages, each message to a corresponding one of the servers S(i). Each message includes it's own corresonding nonce N(i) and not a common nonce associated with a plurality of servers as claimed.

In a specific provided example, each server S(i) sets a state variable indicating that a verification process is pending for its nonce N(i). The server S(i) may then transmit to the recovery client 220 a single message, which is based on both the server response data C(i) and the nonce N(i). The client 220 digitally signs each received message with its private key and returns the message to the corresponding server S(i), where the message is decoded utilizing the user's public key. Upon receipt of an associated message, each server S(i) determines whether the state variable indicates verification of its pending nonce N(i). If verification is pending, then the server verifies that the received proof data successfully demonstrates knowledge of strong secret K and freshness linked to nonce N(i). That is, if the correct nonce is included in the decoded message, then the server S(i) has verified it contributed the correct server secret data b(i) to generate the strong secret data K.

In support of the above interpretation of *Kaliski*, the applicants respectfully point out that the specification makes clear that the designation "i", used throughout the specification, is an index for each of the servers[9]. Moreover, as shown in the Figures, e.g., Fig. 6, which relates to the passages cited and relied upon by the Examiner, each of the dashed boxes 110, 120, 130, 140, and 220 represents one of the components of system 100 or system 200. The solid boxes represent various steps in the two methods

[9] See for example, *Kaliski*, paragraph 25.

300 and 400. The location of a solid box within a dashed box generally indicates that that specific step is performed by that specific component[10]. As shown in Fig. 6, each server S(i), which is represented by server S(1) through S(N) selects its own nonce N(i) at 690. That is, server S(1) selects nonce N(1) while server S(N) selects nonce N(N)[11]. Each server as schematically shown, sends its own message to generate proof data by the recovery client 220 (see 650). Moreover, the recovery client transmits verification data independently back to each server S(i) at 655 as seen by the verify recovery step at 660.

Moreover, *Bartolomeos* in view of *Kaliski* further fails to teach or suggest at least:

> …receiving the common nonce signed by the client at a middle-tier server … and providing the signed common nonce to the plurality of servers as a signature for transactions so as to authenticate the client to the plurality of servers.

As noted above, the invention in *Kaliski* deliberately and expressly avoids any "middle tier" interaction. The express purpose is to keep the strong secret data K only at the client, and to insure that interaction between the client and each secret data server and/or verification server is secure. By routing each signed nonce to a middle-tier server before returning the message to its corresponding verification server would usurp the essence of the invention in *Kaliski*.

Moreover, each signed nonce does not authenticate the client to the plurality of severs. Authentication is performed as a separate step where the generating client authenticates the user[12]. Moreover, the servers use strength properties and unverified recovery attempts to identified non-authorized accesses. Kaliski does not teach or suggest providing a signed common nonce to authenticate the client to a plurality of servers.

In view of the clarifying comments and remarks above, the applicants respectfully request that the rejection to claim 1, and the claims that depend therefrom, be withdrawn.

---

[10] See for example, *Kaliski*, paragraph 51.
[11] See for example, *Kaliski*, paragraph 83.
[12] See for example, *Kaliski*, paragraph 72.

Claims 26 and 27 recite analogous elements (in system and computer program product form) to that described above with reference to claim 1. As such, the arguments set out above apply by analogy. In view of the above, the applicants respectfully request that the rejection of claims 26 and 27 be withdrawn.

With respect to claim 28, *Bartolomeos* in view of *Kaliski* fails to teach or suggest at least:

> A method of authenticating a client, comprising… receiving at a server of a plurality of servers, a common nonce that is provided to each of the plurality of servers from an entity other than the client or the plurality of servers, the common nonce being associated with each of the plurality of servers and signed by the client…

As noted in greater detail above, *Bartolomeos* and *Kaliski,* alone or in combination, fail to teach or suggest a common nonce that is provided to each of a plurality of servers from an entity other than the client or the plurality of servers. In view of the clarifying remarks and comments herein, the applicants respectfully request that the rejection of claim 28 be withdrawn.

Claims 29 and 32 recite analogous elements (in system and computer program product form) to that described above with reference to claim 28. As such, the arguments set out above apply by analogy. In view of the above, the applicants respectfully request that the rejection of claims 29 and 32 be withdrawn.

Claims 4, 6, 12, 13 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Bartolomeos* in view of *Kaliski* in further view of Schneier – Applied Cryptography (hereinafter, '*Schneier*').

The applicants respectfully assert that the above claims are patentable over the cited art by virtue of being dependent upon a base claim that the applicants assert is patentable as set out more fully above. In view of the clarifying remarks herein, the applicants respectfully request that the above rejections are withdrawn.

Claims 16-19, 21 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Bartolomeos* in view of *Kaliski* in further view of Menezes et al. (Handbook of Applied Cryptography). (hereinafter, '*Menezes*').

The applicants respectfully assert that the above claims are patentable over the cited art by virtue of being dependent upon a base claim that the applicants assert is patentable as set out more fully above. In view of the clarifying remarks herein, the applicants respectfully request that the above rejections are withdrawn.

Conclusion

For all of the above reasons, the applicants respectfully submit that the above claims recite allowable subject matter. The Examiner is encouraged to contact the undersigned to resolve efficiently any formal matters or to discuss any aspects of the application or of this response. Otherwise, early notification of allowable subject matter is respectfully solicited.

Respectfully submitted,
Stevens & Showalter, L.L.P.
By /Thomas E. Lees/
Thomas E. Lees Reg. No. 46,867

7019 Corporate Way
Dayton, Ohio 45459-4238
Phone 937-438-6848
Fax 937-438-2124

September 4, 2007